XP-002395976

Windows NT FAQ Single File Version

The Web version of the Windows NT FAQ is at http://www.ntfaq.com. To subscribe to the Windows NT FAQ send a mail to nt-faq@ed-com.com with subscribe in the body of the message to receive the updated single file version of the FAQ once a week.

This single file version of the FAQ is available for download from http://www.ntfaq.com/faqcomp.zip.

Contents

Active Directory

Backups

If you are upgrading a 4.0 domain then during the DCPROMO execution the NetBIOS name cannot be changed. You are stuck with the NetBIOS name of the 4.0 domain but you can of course have a totally different DNS name.

Q. How can I monitor when the Knowledge Consistency Checker (KCC) is run?

A. The KCC which manages the connection objects for inter and intra site replication runs periodically and ascertains if any new objects need creating or existing objects deleted.

If you want you can monitor exactly when its execution starts and finishes by performing the following actions:

1. Start the registry editor (Regedit.exe)
2. Move to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
3. Double click on '1 Knowledge Consistency Checker'
4. Set the value to 3 (or greater) and click OK
5. Close the registry editor (you don't need to restart the machine for this change to take effect)

With this value set to 3 or greater, the KCC will log extra events which you can view using the Event Viewer and viewing the 'Directory Service' branch.

Common and useful events are:

- events 1009 to signify the beginning of KCC check
- events1013 to signify the end of the KCC check
- events 1133 information about the KCC check
- events 1007 to signify the initialization of the KCC
- events 1015 to signify the stopping of the KCC

Q. What backup software is available for Windows NT?

A. Windows NT ships with NTBACKUP.EXE which is suitable for backing up most installations however its features are quite basic, for the larger more complex installations one of the following may be worth a look

- ADSM from http://www.storage.ibm.com/software/adsm/index.htm
- ARCserveIT from http://www.cai.com/arcserveit/
- Back Again II from http://www.cds-inc.com/
- Backup Exec from http://support.veritas.com/index_bottom_Product_Cat_Backup_Exec.htm
- Backup Express from www.syncsort.com
- EaseBackup from http://members.xoom.com/KieProgSoft/
- Legato NetWorker from http://www.legato.com/

- NovaBack+ from http://www.novastor.com
- OpenView OmniBack from http://www.hp.com
- Replica from http://www.stac.com/replica/
- Retrospect 5.0 from www.dantz.com
- UltraBac from http://www.ultrabac.com

Q. How do I add a tape drive?

A. Before you can add a tape drive you should first ensure that the correct SCSI driver is loaded for the card the tape drive is connected to. Once the SCSI driver is loaded you should perform the following

1. Start the Tape Devices control panel applet (Start - Settings - Control Panel - Tape Devices)
2. Click the detect button for NT to detect your tape drive. If this works goto step 5
3. If the drive could not be detected the click the drivers tab
4. Click the Add button and select your tape drive from the list or click the Have Disk button and select the location for the driver.
5. Click OK
6. Restart the computer

Q. What types of backup does NTBACKUP.EXE support?

A. NTBACKUP.EXE supports 5 different types of backups

- Normal backup - Backs up the files selected and marks them as backed up.
- Incremental backup - Backs up files that have changed since the last backup. Once the files have been backed up the files are marked as backed up.
- Differential backup - Same as above, backs up files that have changed since the last backup but does not mark the files as backed up
- Copy backup - Same as a normal backup but does not mark files as backed up
- Daily backup - Backs up selected files that have been modified on that day, the files are not marked as backed up

Q. What backup strategies are available?

A. The main backup strategy is on a weekly plan as follows

- Monday - Incremental backup
- Tuesday - Incremental backup
- Wednesday - Incremental backup
- Thursday - Incremental backup
- Friday - Normal backup

As you know an incremental backup only backs up those files that have changed since the last backup and then sets them as backed up so this type of backup should be quite fast. In the event of a failure you would have to first restore the normal backup and then any subsequent incremental backups.

An alternative would be as follows

- Monday - Differential backup
- Tuesday - Differential backup
- Wednesday - Differential backup
- Thursday - Differential backup
- Friday - Normal backup

Differential backups and incremental backups are the same except that differential does not mark the files as backed up, therefore files backed up on Monday will still be backed up on Tuesday etc. Therefore to restore the backup you would only need to restore the normal backup and the latest differential backup.

It is important to not just have on week's worth of tapes, you should have a tape rotation and have maybe 10 tapes and rotate on a fortnightly basis.

If you wanted an extra backup as a one off you would use a copy backup as this does a full backup but does not mark files as backed up and therefore would not interfere with other backup schemes in use.

Q. What options are available when using NTBACKUP.EXE?

A. Once you start NTBACKUP a list of all drives on the machine will be shown. You can either select a whole drive or double click on the drive and then select directories. Once you have selected the drives/directories click the Backup button.

When performing a backup there are a number of fields that should be completed.

- Current Tape - The name of the inserted tape is shown. You cannot edit this field

- Creation Date - Date the original backup set was created. You cannot edit this field
- Owner - The owner of the tape. You cannot edit this field
- Tape Name - A 32 character string describing the tape
- Operation Append/Replace - If you choose append the new saveset is added to the end of the tape. If you choose replace any information on the current tape is overwritten.
- Verify after backup - If selected once files are copied to tape they are verified against the file on disk
- Backup Local registry - Backs up the computers local registry, you cannot backup remote computers registry's.
- Restrict Access to Owner or Administrator - If you select this tape then the tape is made Secure. Only the owner of the tape or a member of the Administrator or Backup Operators group can access the tape.

Q. Can I run NTBACKUP from the command line?

A. NTBACKUP is fully usable from the command line using the format below

ntbackup <operation> <path> /a /b /d "text" /e /hc:<on/off> /l "<filename>" /r /t <backup type> /tape:n /v

The parameters have the following meanings

<operation>	This will be **backup** . If you wanted to eject a tape you could enter **eject** (but must also include the /tape parameter)
<path>	The list of drives and directories to be backed up. You may not enter file names or use the wildcard character. To backup multiple drives just put a space between them, e.g. **ntbackup backup c: d: etc...**
/a	Append backup sets to the end of the tape. If /a is omitted then the tape will be erased
/b	Backup the local registry
/d "text"	A description of the tape
/e	Logs only exceptions
/hc:<on/off>	If set /hc:on then hardware compression will be used, if /hc:off then no hardware compression will be used.
/l "<filename>"	Location and name for the logfile
/r	Restricts access (ignored if /a is set)
/missingtape	Specifies that a tape is missing from the backup set when the set spans several tapes. Each tape becomes a single unit as opposed to being part of the set.
/t <backup type>	The type of backup, normal, Incremental, Differential, Copy or Daily
/tape:n	Which tape drive to use (from 0 to 9). If omitted tape drive 0 is used
/v	Performs verification

Q. How do I schedule a backup?

A. Before a backup can be scheduled, you must ensure the scheduler service is running on the **target** machine, it does not have to be running on the issuing machine. For information on the schedule service see **Q. How do I schedule commands?**

Once the scheduler service has been started it is possible to submit a backup command using the ntbackup.exe image (image is a name for an executable)

at 22:00 /every:M,T,W,Th,F ntbackup backup d: /v /b

The command above would schedule a backup at 10:00 p.m. on weekdays of drive D: and the local registry with verification.

If you are having problems with the scheduling you may want to use the /interactive switch so in the event of a problem you can interact with the backup program.

Q. How do I restore a backup?

A. To restore a backup saveset is simple and will depend on what was backed up, however the basics are

1. Start NTBACKUP (Start - Administrative Tools - Backup)
2. Double click on the tape unit that has the backup saveset you want. Select the saveset
3. Check the Restore File Permissions if the saveset was backed up off of a NTFS volume
4. Click OK

Q. How do I backup open files?

A. Sometimes files can be corrupted as a backup program will try to backup an open file and when restored the file is

corrupt. To stop NTBACKUP from backing up open files perform the following

1. Start the registry editor
2. Move to HKEY_CURRENT_USER\Software\Microsoft\Ntbackup\Backup Engine
3. Check "Backup files in use". If it is set to 1 double click on the value and set to 0. Click OK
4. Close the registry editor

If you do have "Backup files in use" set to 1 then you should also set the following parameter

HKEY_CURRENT_USER\Software\Microsoft\Ntbackup\User Interface\Skip open files

The values for this are

0 - Do not skip the file, wait till it can be backed up
1 - Skip files that are open/unreadable
2 - Wait for open files to close for **Wait time** (which is another registry value in seconds)

For more information have a look at Q159218 (http://support.microsoft.com/support/kb/articles/q159/2/18.asp)

To backup open files without corruption you should look at Open File Manager software from http://www.stbernard.com (yeah the advert with the cute dog!). You can download a 15 day free trial.

Q. What permissions do I need to perform a backup?

A. The operator performing the backup requires the "back up files and directories" user right. This can be given directly using user manager, or the preferred way is to make the user a member of either the Administrators group or the backup operators group.

Q. How do I backup the registry?

A. Most of the registry hives are open, making them unable to be copied in the normal way, however there are several methods available to you

- If you have a tape drive attached to NT, the NTBACKUP utility will perform a full backup of the registry if you select the "backup local registry" when performing the backup. Please note that NTBACKUP cannot backup registry's on remote machines.
- RDISK /S will backup the registry to the %SystemRoot%/repair directory. RDISK is no longer supplied in Windows 2000, please see **Q. Where is RDISK in Windows 2000?**
- REGBACK.EXE which comes with the resource kit will backup the **open** files that make up the registry, but not the unopened ones, these will need to be manually copied using xcopy.exe or scopy.exe. There is also a utility REGREST.EXE that can be used to restore the registry. To backup the registry to directory d:\regbackup:
  regback d:\regback
- REG.EXE is now supplied with the newer versions of the resource kit and with the BACKUP option, e.g. REG BACKUP you can backup certain sections of the registry to file.

NT does not automatically rename the old Registry to .DA0 as does Windows 95. However, you can use RDISK, the Emergency Recovery Disk utility, to generate fresh duplicates of the Registry, and use this script to keep three old versions on hand:

```
REM REGBACK.BAT note: change M: to home directory on LAN
REM pkzip25 is a product of PKWARE, see www.pkware.com for details
rdisk /s-
if exist m:regback.old del m:regback.old
ren m:regback.sav regback.old
ren m:regback.zip regback.sav
pkzip25 -lev=0 -add -attr=all m:regback %systemroot%\repair\*.*
exit
```

Q. How can I erase a tape using NTBackup that reports errors?

A. When NTBackup starts and when a tape is inserted a scan of the device is performed and if any errors are found one of the following messages will be displayed

- Tape Drive Error Detected.
- Tape Drive Not Responding.
- Bad Tape.

You will not be able to perform any actions on the tape including erasing it. It is possible to force NT to not check a tape when inserted using the /nopoll parameter, e.g.

```
c:\>ntbackup /nopoll
```

You will now be able to erase the tape within NTBackup. If you have multiple tape drives you may want to use the `/tape:n`

parameter to instruct NTBackup to ignore a certain tape drive, otherwise no other parameters should be used.

Once you have erased the tape you should exit ntbackup and restart to use the tape (without specifying /nopoll).

Q. How can I remove a dead submitted Backup process?

A. If you submit a backup using the AT command (the schedule command) and the ntbackup program has a problem, you run Task Manager but are unable to kill the process as an error along the lines of you don't have authority to end the process will be shown. The only solution is to reboot the server.

If you had submitted the ntbackup command with the /interactive switch you would see some kind of error.

Rather than rebooting the server you can create a "special" version of task manager which will be able to kill the rogue NTBACKUP process. Simply submit task manager to start one minute in the future using the AT command or even better using the Resource Kit SOON.EXE utility:

```
C:\> soon 30 /interactive taskmgr
```

In 30 seconds task manager will be displayed and you will be able to kill the NTBACKUP process.

The AT syntax would be

```
C:\> at [\\<computer name>] <time in future> /interactive taskmgr
```

The \\<computer name> is optional and would start Task Manager on another machine.

An alternate method is as follows:

use the TLIST.EXE and the KILL.EXE provided in the Resource kit.

From the command prompt issue...

```
C:\> tlist -t | more
```

The output is .... <snip>

```
ATSVC.EXE (315)
  CMD.EXE (345)
    NTVDM.EXE (348)
    NTBACKUP.EXE (314)
```

(the PID will vary from system to system)
(the "-t" option is important. It provides a tree-like-output to determine which process is the parent and child process)

Use the KILL.EXE to end the parent process CMD.EXE and NTBACKUP.EXE

```
C:\> kill -f 345
```

By killing the parent process it DOES NOT kills the children process it created. Once you kill the CMD.EXE process you then need to kill the children processes that the CMD.EXE called.

Just don't kill the ATSVC.EXE process!!! If you do you no longer have the schedule service running, and you will have to restart it.

You must have Administrative privileges to run the KILL.EXE program.

You may find this better than fumbling with the AT command and waiting for it to start the TASKMGR as a system account.

If this is on a remote server where you can't get to the console load the RKILLSRV.EXE as a service on the remote machine, and use the RKILL.EXE on your local machine. Both programs are from the resource kit. You must have Administrative privileges on the target system to kill the processes.

RKILL.EXE syntax...
Usage : `rkill /view \\servername`
to get the process list on servername
Usage : `rkill /kill \\servername pid`
to kill process pid on servername
Usage : `rkill /token \\servername`
to get your remote security token on servername

Another useful use for this is as part of a scheduled NTBACKUP and to always run the command "kill.exe -f ntbackup.exe" first in the scheduled NTBackup-batch job. I've been told it works great but have never used myself. Basically if there is an old stray backup job running it will kill it first.

Q. What is a batch file?

A. A batch file is just a text file with a .bat or .cmd extension that adheres to a syntax and a set of valid commands/instructions. To run a batch file just enter the name of the file, you don't need to enter the .cmd or .bat extensions. In line with programming tradition the first batch file we write will output "Hello World".

1. Start Notepad
2. Enter the following contents
   @echo hello world
   Echo means output to the screen anything after it (the @ suppresses the command being printed to the screen, try it with and without the @). To stop commands from being displayed in the whole batch file have
   @echo off
   At the top of the batch file.
3. From the file menu select "Save As"
4. Enter a name of "<name>.cmd", make sure you enter the name in quotes or notepad will add .txt to the end!
5. Start a command session (run cmd.exe)
6. Enter the name of the batch file (no extension), e.g.
   testfile

Q. What commands can be used in a batch file?

A. Windows NT 4.0 introduced some extensions to cmd.exe, so to use these make sure HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions is set to 1. The following is a list of the more common commands you will use

call <batch file>	This is used to call one batch from inside another. The execution of the current batch file is suspended until the called batch file completes
exit	Used to stop batch file execution. If a batch file is called from inside another and **exit** is called both batch files are stopped
findstr <string> <filename(s)>	Used to find a string in a file. There are a number of parameters from this and is quite powerful
for	Standard for loop **for /L %n IN (1,1,10) DO @ECHO %n** Would print 1 to 10
goto <label>	Causes the execution of a program to skip to a given point. The actual label name must be preceded with a colon (:), e.g. goto label1 ... :label1 ...
if <condition> ..	The if statement has a great deal of functionality. Some of the more common ones are: **if /i <string1> <compare> <string2> <command>** The /i makes the comparison case insensitive and compare can be one of: EQU equal NEQ not equal LSS less than LEQ less than or equal GTR greater than GEQ greater than or equal **if errorlevel** **if exist <file name>**
rem <string>	A comment
start <window title> <command>	Starts a new command session and runs a given command. Unlike call the execution of the current batch file is not halted and continues

There are some extra utilities supplied with the NT Resource Kit which can be useful.

Q. How can I perform an action depending on the arrival of a file?

A. This is a common request as users on hosts have files FTP'd from a host and need to action it when it arrives. Below is a simple batch file to do this:

```
:filecheck
if exist e:\upload\file.txt goto actionfile
sleep 100
goto filecheck

:actionfile
```